

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division

JASON MONEY and KADRIANA HEISHMAN,  
individually and on behalf of all others similarly  
situated,

Plaintiffs,

v.

INOVA HEALTH SYSTEM,

Defendant.

Case No.:

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiffs Jason Money and Kadriana Heishman (“Plaintiffs”), individually and on behalf of the Class defined below of similarly situated persons, bring this Class Action Complaint and allege the following against Inova Health System (“Inova” or “Defendant”), based upon personal knowledge with respect to Plaintiffs and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

**NATURE OF THE ACTION**

1. Plaintiffs bring this class action against Inova for Inova’s failure to properly secure and safeguard protected health information as defined by the Health Insurance Portability and Accountability Act (“HIPAA”), medical information, and other personally identifiable information, including without limitation names, dates of birth, phone numbers, addresses, financial information, and medical treatment information (collectively, “PII”), for failing to comply with industry standards to protect information systems that contain that PII, and for failing to provide timely, accurate, and adequate notice to Plaintiffs and other Class Members that their PII had been compromised. Plaintiffs seek, among other things, orders requiring Inova to fully and accurately disclose the nature of the information that has been compromised, to adopt reasonably

sufficient security practices and safeguards to prevent incidents like the disclosure in the future, and to provide for the lifetimes of Plaintiffs and Class Members identity theft protective services as Plaintiffs and Class Members will be at an increased risk of identity theft due to the conduct of Inova as described herein.

2. Inova is a leading healthcare provider in the northeastern United States. Inova's 18,000 team members serve over 2 million patients annually in the Washington D.C. metropolitan area through an integrated network of hospitals, primary and specialty care practices, emergency and urgent care centers, outpatient services and destination institutes.<sup>1</sup>

3. On or about September 10, 2020, Inova announced a security incident involving patient PII. (the "Data Breach"). The security incident was "wide-reaching" and compromised the PII of at least 1,045,270 individuals, according to Inova's notice to the U.S. Secretary of Health and Human Services at the Office for Civil Rights.<sup>2</sup>

4. As of September 10, 2020, Inova represented that its investigation is "still ongoing[;]" thus, the number of individuals actually affected may be far greater than 1 million. An exemplar of the Notification of Data Security Incident letter from Inova dated September 10, 2020 (the "Notification Letter") that was sent to Plaintiffs is attached hereto as **Exhibit "A."**

5. This case involves a breach of a computer system by an unknown third party, resulting in the unauthorized disclosure of the PII of Plaintiffs and Class Members by Inova to unknown third parties. As a result of Inova's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII is now in the hands of criminals. Plaintiffs and

---

<sup>1</sup> Inova, About Inova, <https://www.inova.org/about-inova> (last visited Oct. 14, 2020).

<sup>2</sup> Department of Health and Human Services, Office for Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) (last accessed Oct. 14, 2020).

Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiffs and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to Inova's failures.

6. Additionally, as a result of Inova's failure to follow contractually-agreed upon, federally-prescribed, industry standard security procedures, Plaintiffs and Class Members received only a diminished value of the services Inova was to provide. Inova acknowledges that, "[p]atients have the right to privacy and confidentiality about their care, diagnosis and medical information."<sup>3</sup> Defendant expressly represented that, "[e]very patient can expect that his or her privacy will be protected and that patient-specific information [would] be released only to persons as permitted by law or by the patient."<sup>4</sup>

7. In its Privacy Policy, Defendant provided an extensive list and description of situations and reasons why patients' PII might be disclosed to a third party without their written permission—none of which is the case here.<sup>5</sup>

8. Accordingly, Plaintiffs, individually and on behalf of all others similarly situated, allege claims for negligence, breach of contract, breach of implied contract, unjust enrichment, breach of fiduciary duty, breach of confidence, and violation of Virginia state statutes.

### **PARTIES**

9. Plaintiff Jason Money is a citizen and resident of Ashburn Virginia. At all times relevant to this Complaint, Mr. Money was a patient of Inova, whose PII was disclosed without

---

<sup>3</sup>Inova, Code of Conduct, [https://www.inova.org/sites/default/files/for\\_employees/compliance/inova\\_code\\_of\\_conduct\\_2020\\_rev\\_jun1\\_2020.pdf](https://www.inova.org/sites/default/files/for_employees/compliance/inova_code_of_conduct_2020_rev_jun1_2020.pdf) (last accessed Oct. 14, 2020).

<sup>4</sup>*Id.*

<sup>5</sup> Inova, Privacy Policy, <https://www.inova.org/sites/default/files/2019-04/eng-privacy-policy.pdf> (last accessed Oct. 14, 2020).

authorization to an unknown third party as a result of the Data Breach.

10. Plaintiff Kadriana Heishman is a citizen of Virginia, residing in California. At all times relevant to this Complaint, Ms. Heishman was a patient of Inova, whose PII was disclosed without authorization to an unknown third party as a result of the Data Breach.

11. Defendant Inova is the Washington D.C. metro region's leading non-stock, non-profit healthcare system.<sup>6</sup> Inova is incorporated in the Commonwealth of Virginia and its principal address is 8110 Gatehouse Road, Suite 200E, Falls Church, Virginia 22042.

12. Inova cares for patients through a network of hospitals, primary and specialty care practices, emergency care centers, outpatient services, and destination institutes located in the Commonwealth of Virginia and the State of Maryland. Due to the nature of these services, Inova acquires and electronically stores patient PII.

### **JURISDICTION AND VENUE**

13. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a different state from Defendant.

14. This Court has personal jurisdiction over Inova because Inova maintains its principal place of business in this District and is authorized to and does conduct substantial business in this District.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in, was directed to,

---

<sup>6</sup> Inova, Patient and Visitor Information, <https://www.inova.org/patients-visitors> (last accessed Oct. 14, 2020).

and/or emanated from this District, Inova is based in this District, Inova maintains patients' PII in this District, and has caused harm to Plaintiffs and Class Members residing in this District.

### **FACTUAL BACKGROUND**

#### ***A. Inova's Business***

16. Inova was founded in 1956 as the Fairfax Hospital Association, and has grown with its surrounding community and the Washington D.C. region to provide a full spectrum of health services. Inova's mission is to provide "world-class healthcare—every time, every touch—to each person in every community it has the privilege to serve."<sup>7</sup> Inova cares for patients through a network of hospitals, primary and specialty care practices, emergency care centers, outpatient services, and destination institutes.

17. Due to the nature of these services, Inova routinely acquires patient PII.

18. Patients demand security to safeguard their PII. As a healthcare provider, Inova is required to ensure that such private, personal information is not disclosed or disseminated to unauthorized third parties without the patients' express written consent, as further detailed below.

19. Upon information and belief, Inova uses cloud-based storage services provided by a third party vendor to maintain and store patient PII.

20. Businesses, like Inova, save money by using a cloud service for collecting and storing data by not having to pay for the cost of excessive capacity or maintaining the infrastructure required of dedicated server.

---

<sup>7</sup> <https://www.inova.org/about-inova>

21. The primary downside of cloud computing is the increased data security risk inherent in its use.<sup>8</sup>

***B. The Data Breach***

22. Inova received notification on July 16, 2020, that its cloud computing vendor had experienced a security incident compromising Inova's patient information. According to Inova's Notification Letter, an unauthorized third party was able to gain access to the cloud computing platform housing Inova patients' PII between February 7, 2020 and May 20, 2020. The third party not only was able to view Plaintiffs and Class Members' PII, but was able to "intermittently" remove the data from the cloud platform throughout a three month period.

23. After learning of the issue, Inova allegedly commenced an investigation. That investigation is ongoing, but has so far revealed that approximately 1,045,270 individuals were victims of the Data Breach.

24. On August 10, 2020, Inova, either during its own investigation or relying on the investigation commenced by its cloud vendor, determined that the data accessed and removed by the unauthorized third party includes names, addresses, dates of birth, phone numbers, health care provider names, dates of service, hospital departments visited, and philanthropic donation history.

25. Inova attests that the Inova electronic health record system "was not impacted by this incident[,]" yet it fails to explain how the third party gained access to information regarding Plaintiffs and Class Members' health care provider names, dates of service, and hospital departments visited.

---

<sup>8</sup> See, e.g., *12 Risks, Threats, & Vulnerabilities in Moving to the Cloud*, CARNEGIE MELLON UNIVERSITY BLOG (March 5, 2018), available at: [https://insights.sei.cmu.edu/sei\\_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html](https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html)

26. Inova claims that after discovery of the Data Breach, the unauthorized third party was paid a “ransom” in exchange for the assurance that the removed data was permanently deleted. Inova provides no confirmation to Plaintiffs or Class Members that the data was in fact deleted, that it was not distributed to others prior to deletion, or that copies were not made. Instead, Inova asks Plaintiffs and Class Members to rest assured on a thief’s promises.

27. Inova is also “assured” that its cloud vendor has “closed the vulnerability that allowed the incident” in an effort to prevent “incidents like this” from happening in the future. Inova’s Notification Letter provides no particulars regarding how “incidents like this” happened in the first place much less any details as to what steps have been taken with regard to the security of patient data housed on the cloud platform.

28. Inova’s Notification Letter, dated nearly two months after Inova first learned about the Data Breach, was untimely and woefully deficient, failing to provide basic details concerning the Data Breach, including, but not limited to, why sensitive patient information was stored with a cloud computing vendor which clearly did not have adequate security systems, the deficiencies in the security systems that permitted unauthorized access, whether the stolen data was encrypted or otherwise protected, and whether Inova has confirmation that the data has actually been deleted and not otherwise disseminated.

29. Even worse, Inova offered absolutely no identity theft monitoring services to Plaintiffs and Class Members so that Plaintiffs and Class Members can begin to protect themselves from inevitable fraud and identity theft.

30. In deliberate disregard to the fact that the stolen sensitive information was accessed by an unauthorized third party, Inova downplayed the seriousness of the incident by informing Plaintiffs and Class Members that according to its cloud computing vendor, “there is no evidence

to believe that any data will be misused, disseminated, or otherwise made publically available” and that Inova, simply “out of an abundance of caution,” wanted to make Plaintiffs and Class Members aware of the Data Breach.

31. These representations are just boilerplate language pulled off a common template, clearly evidencing Inova’s lack of concern for the seriousness of the Data Breach—wherein an unauthorized third party gained access to Inova’s stored PII and exfiltrated that data for more than three months.

32. Plaintiffs’ and Class Members’ PII is likely for sale to criminals on the dark web, meaning even more unauthorized persons have accessed and viewed Plaintiffs’ and Class Members’ personal information.

### ***C. Inova’s Privacy Policies***

33. Inova makes numerous promises to its patients that it will maintain the security and privacy of their PII.

34. Inova represents in its Code of Conduct that integrity is the “core value of Inova” and it is “central to all that we do.” Inova commits to “consistently upholding the highest moral and ethical standards and to honoring [those] commitments” by providing world class healthcare to each person in every community it serves.<sup>9</sup>

35. Inova also commits to “maintaining the confidentiality of patient information.” Inova instructs its employees not to “use or disclose patient-specific information except when it is permitted or required by law, unless the patient has authorized such disclosure.” Inova admonishes

---

<sup>9</sup>Inova, Code of Conduct, [https://www.inova.org/sites/default/files/for\\_employees/compliance/inova\\_code\\_of\\_conduct\\_2020\\_rev\\_jun1\\_2020.pdf](https://www.inova.org/sites/default/files/for_employees/compliance/inova_code_of_conduct_2020_rev_jun1_2020.pdf) (last accessed Oct. 14, 2020).

its employees to “never use or disclose confidential information in a manner that violates the privacy rights of [its] patients.”<sup>10</sup>

36. Inova promises that “every patient can expect that his or her privacy will be protected and that patient-specific information will be released only to persons as permitted by law or by the patient.”<sup>11</sup>

37. Inova provides in its “Notice of Privacy Practices” various situations and circumstances in which it uses and discloses PII, none of which describe the facts involved in the Data Breach.<sup>12</sup>

38. Inova created these policies, representations, and requirements, and publicly advertised them on its website as a means of increasing the value of its relationships with patients, thus allowing it to charge consumers higher rates under the guise of enhanced security and information security practices. These agreements were the same for all of Inova’s patients, including Plaintiffs and Class Members.

#### ***D. The Healthcare Sector is Particularly Susceptible to Data Breaches***

39. Inova was on notice that companies in the healthcare industry are targets for data breaches.

40. Inova was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that “[t]he FBI has observed malicious actors targeting healthcare related systems,

---

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*

<sup>12</sup> Inova, Privacy Policy, <https://www.inova.org/sites/default/files/2019-04/eng-privacy-policy.pdf> (last accessed Oct. 14, 2020).

perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII).”<sup>13</sup>

41. The American Medical Association (“AMA”) has also warned healthcare companies about the importance of protecting their patients’ confidential information:

Cybersecurity is not just a technical issue; it’s a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients’ health and financial information, but also patient access to care.<sup>14</sup>

42. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.<sup>15</sup> In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.<sup>16</sup> That trend continues.

43. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.<sup>17</sup> Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A

---

<sup>13</sup> Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), available at: <https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820> (last accessed Sept. 27, 2020).

<sup>14</sup> Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass’n (Oct. 4, 2019), available at: <https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals> (last visited Sept. 27, 2020).

<sup>15</sup> Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), available at: <https://www.idtheftcenter.org/surveys-studys> (last accessed Sept. 27, 2020).

<sup>16</sup> Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, available at: <https://www.idtheftcenter.org/2017-data-breaches/> (last accessed Sept. 18, 2020).

<sup>17</sup> Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, available at: <https://www.idtheftcenter.org/2018-data-breaches/> (last accessed Sept. 18, 2020).

report focusing on healthcare breaches found that the “average total cost to resolve an identity theft-related incident . . . came to about \$20,000,” and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.<sup>18</sup> Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.<sup>19</sup>

44. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by “bad actors” such as cybercriminals.<sup>20</sup> “Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.”<sup>21</sup>

45. Moreover, Inova had a heightened awareness of its susceptibility to data breaches. In

---

<sup>18</sup> Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), available at: <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last accessed Sept. 28, 2020).

<sup>19</sup> *Id.*

<sup>20</sup> 2019 HIMSS Cybersecurity Survey, available at: <https://www.himss.org/2019-himss-cybersecurity-survey> (last accessed Sept. 28, 2020).

<sup>21</sup> Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, available at: <https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks> (last accessed Sept. 28, 2020).

2018, two years prior to the breach that is the subject of this action, Inova informed 12,331 patients that a hacker had infiltrated its system and accessed personal health data.<sup>22</sup> The breached data in 2018 included patient names, addresses, dates of birth, medical records, and Social Security numbers. Upon information and belief, 2018 was at least Inova's second data breach involving patient information. Given the company's history, Inova should have been aware that it was and continues to be a target for cyber attacks and therefore must maintain adequate security measures.

46. As the number of healthcare data breaches continues to rise, a commonly identified vulnerability is a misconfigured cloud server, which leaves a healthcare organization wide open to a data breach.<sup>23</sup>

47. As a healthcare provider, Inova knew, or should have known, the importance of safeguarding the patients' PII entrusted to it and of the foreseeable consequences if that data was disclosed. This includes the significant costs that would be imposed on Inova's patients as a result of a breach. Inova failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

***E. Inova Obtains, Collects, and Uses a Third Party Vendor to Store Plaintiffs' and Class Members' PII***

48. Inova acquires, collects, and uses cloud-based storage to maintain a massive amount of its patients' protected health information and personally identifiable data.

49. As a condition of engaging in health services, Inova requires that patients entrust it

---

<sup>22</sup> Health IT Security, 12K Patient Billing Records Breached at Inova Health System, Nov. 15, 2018, available at <https://healthitsecurity.com/news/ransomware-attack-on-may-eye-care-breaches-30k-patient-records> (last accessed Oct. 14, 2020).

<sup>23</sup> Atlantic.Net Blog, *Data Breaches Caused by Misconfigured Servers Within a Healthcare Environment*, September 2, 2019, available at: <https://www.atlantic.net/hipaa-data-centers/data-breaches-caused-by-misconfigured-servers-within-a-healthcare-environment/> (last accessed Oct. 10, 2020).

with highly confidential PII.

50. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Inova assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs and Class Members' PII from disclosure.

51. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and, as current and former patients, they rely on Inova to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

***F. The Value of Private Information and the Effects of Unauthorized Disclosure***

52. PII is a valuable commodity to identity thieves. Inova was well aware that the protected health information and personally identifiable information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

53. PII is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.<sup>24</sup> Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and other protected health information on multiple underground Internet websites, commonly referred to as the dark web.

54. While credit card information and associated personally identifiable information can sell for as little as \$1-\$2 on the black market, protected health information can sell for as much

---

<sup>24</sup> Federal Trade Commission, *Warning Signs of Identity Theft*, available at: <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last accessed Sept. 28, 2020).

as \$363 according to the Infosec Institute.<sup>25</sup>

55. Protected health information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

56. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."<sup>26</sup>

57. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

Cyber criminals are selling [medical] information on the black market at a rate of \$50 for each partial EHR, compared to \$1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

58. The ramifications of Inova's failure to keep its patients' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may

---

<sup>25</sup> Center for Internet Security, *Data Breaches: In the Healthcare Sector*, available at: <https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/> (last accessed Sept. 27, 2020).

<sup>26</sup> Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, available at: <https://khn.org/news/rise-of-indentity-theft/> (last visited Sept. 27, 2020).

continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

59. Further, criminals often trade stolen PII on the “cyber black-market” for years following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publicly available.

60. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.<sup>27</sup> This gives thieves ample time to seek multiple treatments under the victim’s name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.<sup>28</sup>

61. Breaches are particularly serious in healthcare industries. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.<sup>29</sup> Indeed, when compromised, healthcare related data is among the most private and personally consequential. A report focusing on healthcare breaches found that the “average total cost to resolve an identity theft-related incident . . . came to about \$20,000,” and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.<sup>30</sup> Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event.

---

<sup>27</sup> See Medical ID Theft Checklist, available at: <https://www.identityforce.com/blog/medical-id-theft-checklist-2> (last accessed Sept. 27, 2020).

<sup>28</sup> Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches* (“Potential Damages”), available at: <https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf> (last accesses Sept. 27, 2020).

<sup>29</sup> Identity Theft Resource Center, *2018 End -of-Year Data Breach Report*, available at: <https://notified.idtheftcenter.org/s/resource> (last accessed Sept.27, 2020).

<sup>30</sup> Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), available at: <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last accessed Sept. 27, 2020); see also, National Survey on Medical Identity Theft, Feb. 22, 2010, cited at p. 2.

Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.<sup>31</sup>

62. Inova knew, or should have known, the importance of safeguarding its patients' PII entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Inova's patients as a result of a breach. Inova failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

63. The ramifications of Inova's failure to keep its patients' protected health information and other PII secure are long lasting and severe.

***G. Defendant's Data Breach Exposed Plaintiffs to Identity Theft and Monetary Injuries***

64. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

65. Despite all of the publicly available knowledge of the continued compromises of PII, Inova's approach to maintaining the privacy of Inova's patients' protected health information and other PII was lackadaisical, cavalier, reckless, or in the very least, negligent.

66. In all manners of life in this country, time has constantly been recognized as compensable, for many people it is the way they are compensated. Plaintiffs and Class Members should be free of having to deal with the consequences of Inova's slippage.

---

<sup>31</sup> *Id.*

#### ***H. Inova's Conduct Violates HIPAA***

67. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services (“HHS”) create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

68. Inova's Data Breach resulted from a combination of insufficiencies that indicate Inova failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Inova's Data Breach that Inova either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiffs' and Class Members' PII.

69. In addition, Inova's Data Breach could have been prevented if Inova implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PII when it was no longer necessary and/or had honored its obligations to its patients.

70. Inova's security failures also include, but are not limited to:

- a. Failing to maintain an adequate data security system to prevent data loss;
- b. Failing to mitigate the risks of a data breach and loss of data;
- c. Failing to ensure the confidentiality and integrity of electronic protected health information Inova creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);
- d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in

violation of 45 CFR 164.312(a)(1);

- e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);
- f. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);
- g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);
- h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);
- i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94);
- j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*

71. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay

and *in no case later than 60 days following discovery of the breach.*”<sup>32</sup>

72. Because Inova has failed to comply with industry standards, while monetary relief may cure some of Plaintiffs’ and Class Members’ injuries, injunctive relief is necessary to ensure Inova’s approach to information security is adequate and appropriate. Inova still maintains the protected health information and other PII of Plaintiffs and Class Members; and without the supervision of the Court via injunctive relief, Plaintiffs and Class Members’ protected health information and other PII remains at risk of subsequent Data Breaches.

### ***I. Inova Failed to Comply with FTC Guidelines***

73. Inova was also prohibited by the Federal Trade Commission Act (“FTC Act”) (15 U.S.C. §45) from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The Federal Trade Commission (“FTC”) has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

74. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.<sup>33</sup>

75. In 2016, the FTC updated its publication, *Protecting Personal Information: A*

---

<sup>32</sup> Breach Notification Rule, U.S. Dep’t of Health & Human Services, *available at: [hhs.gov/hipaa/for-professionals/breach-notification/index.html](https://hhs.gov/hipaa/for-professionals/breach-notification/index.html)* (emphasis added) (last visited Oct. 13, 2020).

<sup>33</sup> Federal Trade Commission, *Start With Security: A Guide for Business*, *available at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>* (last accessed Sept. 27, 2020).

*Guide for Business*, which established cybersecurity guidelines for businesses.<sup>34</sup> The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

76. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.<sup>35</sup>

77. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

78. Inova failed to properly implement basic data security practices. Inova's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

---

<sup>34</sup> Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at: [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last accessed Sept. 27, 2020).

<sup>35</sup> FTC, *Start With Security*, *supra* note 16.

79. Inova was at all times fully aware of its obligation to protect the PII of patients because of its position as a leading healthcare provider. Inova was also aware of the significant repercussions that would result from its failure to do so.

***J. Plaintiffs and Class Members Suffered Damages.***

80. The ramifications of Inova's failure to keep patients' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.<sup>36</sup>

81. Inova's delay in identifying and reporting the Data Breach caused additional harm to Plaintiffs and Class Members. Although their PII was improperly exposed as early as February 7, 2020, Plaintiffs and Class Members were not notified of the Data Breach until September 10, 2020, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

82. As a result of a result of Inova's failure to prevent the Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at increased risk of suffering:

- a. Actual identity theft;
- b. Unauthorized use and misuse of their PII;
- c. The loss of the opportunity to control how their PII is used;
- d. The diminution in value of their PII;
- e. The compromise, publication, and/or theft of their PII;

---

<sup>36</sup> 2014 LexisNexis True Cost of Fraud Study, available at: <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf> (last accessed Sept. 27, 2020).

- f. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- g. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- h. Costs associated with placing freezes on credit reports;
- i. Delay in receipt of tax refund monies;
- j. The diminished value of Inova's goods and services they received;
- k. Lost opportunity and benefits of electronically filing of income tax returns;
- l. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;
- m. The continued risk to their PII, which remains in the possession of Inova and is subject to further breaches so long as Inova fails to undertake appropriate measures to protect the PII in its possession; and
- n. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

### **CLASS ACTION ALLEGATIONS**

83. Plaintiffs bring this suit as a class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civile Procedure.

84. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

**All individuals in the United States whose PII was compromised in the Data Breach first announced by Inova on or about September 10, 2020.**

85. In the alternative to the Nationwide Class, Plaintiffs seek certification of the following Virginia sub-class, defined as follows:

**All individuals residing in Virginia whose PII was compromised in the Data Disclosure first announced by Inova on or about September 10, 2020.**

86. Excluded from the Class are the officers, directors, and legal representatives of Inova, and the judges and court personnel in this case and any members of their immediate families.

87. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

88. Numerosity. Fed. R. Civ. P. 23(a)(1): The Class Members are so numerous that joinder of all Members is impractical. In its report to the U.S. Department of Health and Human Services - Office for Civil Rights, Inova attested that the Data Breach affected at least 1,045,270 patients. Inova has indicated to Plaintiffs and Class Members that it is still working on its investigation, thus the actual number of affected patients may be exponentially higher.

89. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether and to what extent Defendant had a duty to protect the PII of Class Members;
- b. Whether Defendant was negligent in collecting and storing Plaintiffs' and Class

Members' PII;

- c. Whether Defendant had duties not to disclose the PII of Class Members to unauthorized third parties;
- d. Whether Defendant took reasonable steps and measures to safeguard Plaintiffs' and Class Members' PII;
- e. Whether Defendant failed to adequately safeguard the PII of Class Members;
- f. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiffs' and Class Members' PII by storing that information on computers and hard drives in the manner alleged herein, including failing to comply with industry standards;
- g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- h. Whether implied or express contracts existed between Defendant, on the one hand, and Plaintiffs and Class Members on the other;
- i. Whether Defendant had respective duties not to use the PII of Class Members for non-business purposes;
- j. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;
- k. Whether Plaintiffs and Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Defendant's wrongful conduct;
- o. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

- p. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach; and
- q. Whether Plaintiffs and Class Members are entitled to identity theft protection for their respective lifetimes.

90. Typicality. Fed. R. Civ. P. 23(a). Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was disclosed by Inova. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct of Inova. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

91. Policies Generally Applicable to the Class. This class action is also appropriate for certification because Inova has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Inova's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Inova's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

92. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the Class in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiffs have retained

counsel experienced in complex consumer class action litigation and in particular privacy class litigation, and Plaintiffs intends to prosecute this action vigorously.

93. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like Inova. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

94. The nature of this action and the nature of laws available to Plaintiffs and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and the Class for the wrongs alleged because Inova would necessarily gain an unconscionable advantage since Inova would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

95. The litigation of the claims brought herein is manageable. Inova's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

96. Adequate notice can be given to Class Members directly using information maintained in Inova's records.

97. Unless a Class-wide injunction is issued, Inova may continue in its failure to properly secure the PII of Class Members, Inova may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Inova may continue to act unlawfully as set forth in this Complaint.

98. Further, Inova has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under the Federal Rules of Civil Procedure.

**FIRST CAUSE OF ACTION**  
**Negligence**  
**(On Behalf of Plaintiffs and the Class)**

99. Plaintiffs restate and reallege paragraphs 1 through 97 above as if fully set forth herein.

100. As a condition of their utilizing the services of Inova, patients were obligated to provide Inova with certain PII, including their dates of birth, mailing addresses, phone numbers, personal medical information, and other protected health information.

101. Plaintiffs and the Class Members entrusted their PII to Inova on the premise and with the understanding that Inova would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

102. Inova has full knowledge of the sensitivity of PII and the types of harm that Plaintiffs and Class Members could and would suffer if PII was wrongfully disclosed.

103. Inova knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of patients' PII involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

104. Inova had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Inova's security protocols to ensure that Plaintiffs' and Class Members' information in Inova's possession was adequately secured and protected, and that vendors tasked with maintaining such information were adequately trained on security measures regarding the security of patients' personal and medical information.

105. Inova had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and Class Members' PII.

106. Additionally, violations of statutes which establish a duty to take precautions to protect a particular class of persons from a particular injury or type of injury may constitute negligence *per se*.

107. Section 5 of the FTC Act prohibits ““unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Inova, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Inova's duty in this regard.

108. Inova violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII and not complying with applicable industry standards,

as described in detail herein. Inova's conduct was particularly unreasonable given the nature and amount of PII they obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiffs and Class Members.

109. Inova's violation of Section 5 of the FTC Act constitutes negligence *per se*.

110. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

111. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

112. Inova's violation of HIPAA also independently constitutes negligence *per se*.

113. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

114. Plaintiffs and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

115. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

116. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class Members was reasonably foreseeable, particularly in light of the growing amount of data

breaches for health care providers and other industries.

117. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Inova knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and that it had inadequate employee training and education and IT security protocols in place to secure the PII of Plaintiffs and the Class.

118. Inova's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Inova's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Inova's misconduct also included its decisions not to comply with industry standards for the safekeeping and unauthorized disclosure of the PII of Plaintiffs and Class Members.

119. Plaintiffs and the Class Members had no ability to protect their PII that was in Inova's possession.

120. Inova was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

121. Inova had and continues to have a duty to adequately disclose that the PII of Plaintiffs and Class Members within Inova's possession might have been compromised, how it was compromised, and precisely the types of information that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

122. Inova has admitted that the PII of Plaintiffs and Class Members was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

123. Inova, through its actions and/or omissions, unlawfully breached Inova's duties to

Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and Class Members during the time the PII was within Inova's possession or control.

124. Inova improperly and inadequately safeguarded the PII of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

125. Inova failed to heed industry warnings and alerts to provide adequate safeguards to protect patients' PII in the face of increased risk of theft.

126. Inova, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its patients' PII.

127. Inova, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

128. But for Inova's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII of Plaintiffs and Class Members would not have been compromised.

129. There is a close causal connection between Inova's failure to implement security measures to protect the PII of current and former patients and the harm suffered or risk of imminent harm suffered by Plaintiffs and the Class. Plaintiffs' and Class Members' PII was stolen and accessed as the proximate result of Inova's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

130. As a direct and proximate result of Inova's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft;

(ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Inova's possession and is subject to further unauthorized disclosures so long as Inova fails to undertake appropriate and adequate measures to protect the PII of patients and former patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Inova's goods and services Plaintiffs and Class Members received.

131. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

**SECOND CAUSE OF ACTION**  
**Breach of Contract**  
**(On Behalf of Plaintiffs and the Class)**

132. Plaintiffs restate and reallege paragraphs 1 through 97 above as if fully set forth herein.

133. As a healthcare provider, Inova entered into contracts with Plaintiffs and Class Members.

134. The promises and representations described above relating to HIPAA and other industry practices, and about Inova's purported concern about its patients' privacy rights became terms of the contract between Inova and its patients, including Plaintiffs and Class Members.

135. Inova breached these promises by failing to comply with HIPAA and other reasonable industry practices.

136. Plaintiffs and Class Members fully performed their obligations under the contracts with Inova. Inova breached its agreements with Plaintiffs and Class Members by failing to protect their PII. Specifically, Inova: (1) failed to take reasonable steps to use safe and secure systems to protect PII; (2) failed to have appropriate security protocols and measures in place; (3) allowed unauthorized third parties to gain access to patients' PII; and (4) failed to promptly alert or give notice of the Data Disclosure to Plaintiffs and Class Members.

137. As a result of Inova's breach of these terms, Plaintiffs and Class Members have been harmed and put at risk of future harm.

138. Plaintiffs and Class Members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

**THIRD CAUSE OF ACTION  
Breach of Implied Contract  
(On Behalf of Plaintiffs and the Class)**

139. Plaintiffs restate and reallege paragraphs 1 through 97 above as if fully set forth herein.

140. Plaintiffs and Class Members were required to provide their PII, including names, addresses, dates of birth, medical histories, and other personal information to Inova as a condition of their use of Inova's services.

141. Plaintiffs and Class Members paid money to Inova in exchange for goods and services, as well as Inova's promises to protect their protected health information and other PII from unauthorized disclosure.

142. In its written privacy policy, Defendant expressly promised Plaintiffs and Class Members that Defendant would only disclose protected health information and other PII under certain circumstances, none of which relate to the Data Breach.

143. Defendant promised to comply with HIPAA standards and to make sure that Plaintiffs' and Class Members' protected health information and other PII would remain protected.

144. Implicit in the agreement between Inova's patients, including Plaintiffs and Class Members, to provide protected health information and other PII, and Inova's acceptance of such protected health information and other PII, was Inova's obligation to use the PII of its patients for business purposes only, take reasonable steps to secure and safeguard that protected health information and other PII, and not make unauthorized disclosures of the protected health information and other PII to unauthorized third parties.

145. Further, implicit in the agreement, Inova was obligated to provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their protected health information and other PII.

146. Without such implied contracts, Plaintiffs and Class Members would not have provided their protected health information and other PII to Inova.

147. Inova had an implied duty to reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses.

148. Additionally, Inova implicitly promised to retain this PII only under conditions that kept such information secure and confidential.

149. Plaintiffs and Class Members fully performed their obligations under the implied contract with Inova; however, Inova did not.

150. Inova breached the implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs and Class Members' PII, which was compromised as a result of the Data Breach.

151. Inova further breached the implied contracts with Plaintiffs' and Class Members by failing to comply with its promise to abide by HIPAA.

152. Inova further breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Inova created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

153. Inova further breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

154. Inova further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

155. Inova further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

156. Inova further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity

of electronic protected health information in violation of 45 CFR 164.306(a)(2).

157. Inova further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

158. Inova further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations in violation of 45 CFR 164.306(a)(94).

159. Inova further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*

160. Inova further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

161. Inova further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PII.

162. Inova's failures to meet these promises constitute breaches of the implied contracts.

163. Because Inova allowed unauthorized access to Plaintiffs' and Class Members' PII and failed to safeguard the PII, Inova breached its contracts with Plaintiffs and Class Members.

164. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide accurate and complete PII and to pay Inova in exchange for Inova's agreement to, *inter alia*, protect their PII.

165. Inova breached its contracts by not meeting the minimum level of protection of Plaintiffs' and Class Members' protected health information and other PII, because Defendant did not prevent against the breach of over 1 million patients' PII.

166. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Inova providing goods and services to Plaintiffs and Class Members that were of a diminished value.

167. As a direct and proximate result of Inova's breach of its implied contracts with Inova and Class Members, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Inova's possession and is subject to further unauthorized disclosures so long as Inova fails to undertake appropriate and adequate measures to protect the PII of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Inova's goods and services they received.

168. As a direct and proximate result of Inova's breach of its implied contracts with

Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

**FOURTH CAUSE OF ACTION  
Unjust Enrichment  
(On Behalf of Plaintiffs and the Class)**

169. Plaintiffs restate and reallege paragraphs 1 through 97 above as if fully set forth herein.

170. Plaintiffs and Class Members conferred a monetary benefit on Inova. Specifically, they purchased goods and services from Inova and provided Inova with their PII. In exchange, Plaintiffs and Class Members should have received from Inova the goods and services that were the subject of the transaction and should have been entitled to have Inova protect their PII with adequate data security.

171. Inova knew that Plaintiffs and Class Members conferred a benefit on Inova and accepted and have accepted or retained that benefit. Inova profited from the purchases and used the PII of Plaintiffs and Class Members for business purposes.

172. The amounts Plaintiffs and Class Members paid for Inova's goods and services were used, in part, to pay for the administrative costs of data management and security.

173. Under the principles of equity and good conscience, Inova should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Inova failed to implement the data management and security measures that are mandated by industry standards.

174. Inova failed to secure the PII of Plaintiffs and Class Members and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

175. Inova acquired the PII through inequitable means in that Inova failed to disclose

the inadequate security practices previously alleged.

176. If Plaintiffs and Class Members knew that Inova would not secure their PII using adequate security, they would not have used the services of Inova.

177. Plaintiffs and Class Members have no adequate remedy at law.

178. As a direct and proximate result of Inova's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Inova's possession and is subject to further unauthorized disclosures so long as Inova fails to undertake appropriate and adequate measures to protect the PII of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Inova's goods and services they received.

179. As a direct and proximate result of Inova's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

180. Inova should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that Inova unjustly received from them. In the alternative, Inova should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Inova's goods and services.

**FIFTH CAUSE OF ACTION  
Breach of Fiduciary Duty  
(On Behalf of Plaintiffs and the Class)**

181. Plaintiffs restate and reallege paragraphs 1 through 97 above as if fully set forth herein.

182. In light of the special relationship between Inova and its patients, whereby Inova became a guardian of Plaintiffs' and Class Members' highly sensitive, confidential, personal, financial information, and other PII, Inova was a fiduciary, created by its undertaking and guardianship of the PII, to act primarily for the benefit of its patients, including Plaintiffs and Class Members, for: (1) the safeguarding of Plaintiffs' and Class Members' PII; (2) timely notifying Plaintiffs and Class Members of a data breach or disclosure; and (3) maintaining complete and accurate records of what and where Inova's patients' information was and is stored.

183. Inova had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its patients' relationship, in particular to keep secure the PII of its patients.

184. Inova breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently investigate the Data Breach to determine the number of Members affected in a reasonable and practicable period of time.

185. Inova breached its fiduciary duties to Plaintiffs and Class Members by failing to protect Plaintiffs' and Class Members' protected health information and other PII.

186. Inova breached its fiduciary duties to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

187. Inova breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Inova created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

188. Inova breached its fiduciary duties to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

189. Inova breached its fiduciary duties to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

190. Inova breached its fiduciary duties to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

191. Inova breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

192. Inova breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

193. Inova breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 CFR 164.306(a)(94).

194. Inova breached its fiduciary duties to Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*

195. Inova breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PII.

196. As a direct and proximate result of Inova's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Inova's possession and is subject to further unauthorized disclosures so long as Inova fails to undertake appropriate and adequate measures to protect the PII of customers/patients and former customers/patients in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Inova's goods and services they

received.

197. As a direct and proximate result of Inova's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

**SIXTH CAUSE OF ACTION**  
**Violation of Virginia's Personal Information Breach Notification Act**  
*Va. Code Ann. §§ 18.2-186.6, et seq.*  
**(On Behalf of Plaintiffs and the Virginia Subclass)**

198. Plaintiffs restate and reallege paragraphs 1 through 97 above as if fully set forth herein.

199. Inova is required to accurately notify Plaintiffs and Virginia Subclass members following discovery or notification of a breach of their data security system if unencrypted or unredacted PII was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identity theft or another fraud, without reasonable delay under Va. Code Ann. § 18.2-186.6(B).

200. Inova is an entity that maintains computerized data that includes PII as defined by Va. Code Ann. §§ 18.2-186.6(B), (D).

201. Plaintiffs and Virginia Subclass members' PII includes personal information as covered under Va. Code Ann. § 18.2-186.6(A).

202. Because Inova discovered a breach of its security system in which unencrypted or unredacted PII was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identity theft or

other fraud, Inova had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Va. Code Ann. §§ 18.2-186.6(B), (D).

203. By failing to disclose the Data Breach in a timely and accurate manner, Inova violated Va. Code Ann. §§ 18.2-186.6(B), (D).

204. As a direct and proximate result of Inova's violations of Va. Code Ann. §§ 18.2-186.6(B), (D), Plaintiffs and Virginia Subclass members suffered damages as described above.

205. Plaintiffs and Virginia Subclass members seek relief under Va. Code Ann. § 18.2-186.6(I), including actual damages.

**SEVENTH CAUSE OF ACTION**  
**Violation of the Virginia Health Records Privacy Act**  
*Va. Code § 32.1-127.1:03*  
**(On Behalf of Plaintiffs and the Class)**

206. Plaintiffs restate and reallege paragraphs 1 through 97 above as if fully set forth herein.

207. The Virginia Health Records Privacy Act ("VHRPA") recognizes an individual's right of privacy in the content of his health records.

208. Under the VHRPA, "no health care entity...may disclose an individual's health records" without permission from the patient or other legal authorization. Va. Code § 32.1-127.1:03(A).

209. Inova is a healthcare entity subject to the provisions of the VHRPA. Va. Code § 32.1-127.1:03(B).

210. Plaintiffs' and Class Members' records containing their PII fall within the ambit of the VHRPA because they are "written, printed or electronically recorded material maintained by

a health care entity in the course of providing health services to an individual concerning the individual and the services provided.” Va. Code § 32.1-127.1:03(B).

211. Plaintiffs and Class Members had a legitimate expectation of privacy with respect to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

212. Inova owed a duty to its patients, including Plaintiffs and Class Members, to keep their PII confidential.

213. Inova failed to protect and allowed unauthorized and unknown third parties unfettered access to the PII of Plaintiffs and Class Members.

214. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and Class Members, especially where the information includes medical information, is highly offensive to a reasonable person.

215. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII to Inova as part of their use of Inova’s services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

216. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiffs and Class Members was disclosed to and used by third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

217. Inova’s wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Inova can be viewed, distributed, and

used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

**EIGHTH CAUSE OF ACTION  
INJUNCTIVE/DECLARATORY RELIEF  
(On Behalf of Plaintiffs and the Nationwide Class)**

218. Plaintiffs restate and reallege paragraphs 1 through 97 as if fully set forth herein.

219. This cause of action is brought under the federal Declaratory Judgment Act, 28 U.S.C. § 2201.

220. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Inova to provide adequate security for the PII they collected from Plaintiffs and Class Members.

221. Inova owe a duty of care to Plaintiffs and Class Members requiring them to adequately secure PII.

222. Inova still possesses PII regarding Plaintiffs and Class Members.

223. Since the Data Breach, Inova has announced no specific changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent further attacks.

224. Inova has not satisfied their contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Inova's insufficient data security is known to hackers, the PII in Inova's possession is even more vulnerable to cyberattack.

225. Actual harm has arisen in the wake of the Data Breach regarding Inova's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to

the exposure of their PII and Inova's failure to address the security failings that lead to such exposure.

226. There is no reason to believe that Inova's security measures are any more adequate now than they were before the Data Breach to meet Inova's contractual obligations and legal duties.

227. Plaintiffs, therefore, seek a declaration (1) that Inova's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Inova must implement and maintain reasonable security measures, including, but not limited to, the following:

- a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
- c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;
- d. Ordering that Defendant segment patient data by, among other things, creating firewalls and access controls so that if one area of Defendant's system is compromised, hackers cannot gain access to other portions of Defendant's systems;
- e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner patient data not necessary for its provisions of services;

- f. Ordering that Defendant conduct regular computer system scanning and security checks;
- g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- h. Ordering Defendant to meaningfully educate its current, former, and prospective patients about the threats it faces as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

**PRAYER FOR RELIEF**

WHEREFORE Plaintiffs on behalf of themselves and all others similarly situated, pray for relief as follows:

- a. For an Order certifying the Class as defined herein, and appointing Plaintiffs and his Counsel to represent the Class;
- b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;
- c. For equitable relief compelling Defendant to use appropriate cyber security methods and policies with respect to PII collection, storage, and protection, and to disclose with specificity to Class Members the type of PII compromised;
- d. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;
- e. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

- f. For prejudgment interest on all amounts awarded; and
- g. Such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: October 15, 2020

Respectfully submitted,

By: /s/ Steven T. Webster  
Steven T. Webster (VSB No. 31975)  
**WEBSTER BOOK LLP**  
300 N. Washington Street, Suite 404  
Alexandria, Virginia 22314  
Tel: (888) 987-9991  
swebster@websterbook.com

*Plaintiffs' Local Counsel*

JEAN S. MARTIN\*  
FRANCESCA KESTER\*  
**MORGAN & MORGAN**  
**COMPLEX LITIGATION GROUP**  
201 N. Franklin Street, 7th Floor  
Tampa, Florida 33602  
Telephone: (813) 223-5505  
Facsimile: (813) 223-5402  
jeanmartin@forthepeople.com  
fkester@forthepeople.com

WILLIAM 'BILLY' PEERCE HOWARD\*  
HEATHER H. JONES\*  
**THE CONSUMER PROTECTION FIRM**  
4030 Henderson Boulevard  
Tampa, FL 33629  
(813) 500-1500  
Billy@TheConsumerProtectionFirm.com  
Heather@TheConsumerProtectionFirm.com

M. ANDERSON BERRY\*  
LESLIE GUILLON\*  
**CLAYEO C. ARNOLD,**  
**A PROFESSIONAL LAW CORP.**

865 Howe Avenue  
Sacramento, CA 95825  
(916) 777-7777  
aberry@justice4you.com  
lguillon@justice4you.com

*\* Pro Hac Vice applications to be submitted*

*Attorneys for Plaintiffs and the Proposed Class*